BAB III

SANDI LINIER DAN SANDI GRUP

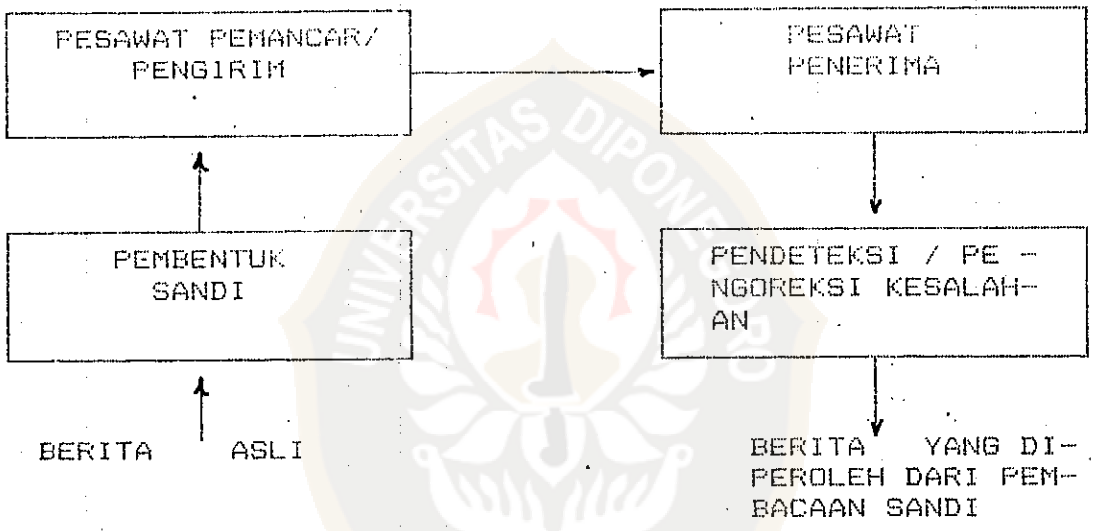
3.1. TRANSMISI SANDI LINIER PADA CHANNEL SIMETRIS BINER

Pada masalah sandi ini akan dibahas suatu applikasi bidang Aljabar modern, yang merupakan salah satu cabang ilmu Matematika, yang mempunyai peranan penting. Mengingat pentingnya masalah keamanan/ keselamatan transmisi dari suatu berita melalui suatu channel dapat dipengaruhi oleh gangguan.

Berita tersebut ditransmisikan dalam bentuk sinyal-sinyal dalam suatu channel. Dan sinyal-sinyal yang ada dipermukaan di muka bumi ini ditransmisikan oleh berbagai macam channel. Berbagai macam channel tersebut meliputi sinyal radio dari suatu satelit ruang angkasa atau dari suatu tempat yang jauh dipermukaan bumi, sinyal-sinyal telepon kabel atau telepon gelombang pendek, atau transmisi informasi diantara memori dengan CPU dari suatu komputer. Dari jaringan-jaringan transmisi tersebut, besar kemungkinan akan mendapat gangguan,yaitu dari sinyal-sinyal yang tak ada hubungannya dengan informasi yang ditransmisikan, sehingga dapat merubah isi informasi yang ditransmisikan.

Pada sebagian besar komputer dan sistem komunikasi, infomasi yang ditransmisikan berupa bilangan-bilangan biner yaitu bilangan 0 dan 1. Dari

informasi-informasi yang ditransmisikan berupa sinyal-sinyal tersebut, beberapa diantaranya diterima berisi kesalahan dan perlu diadakan pendeteksian dan selanjutnya mengoreksi informasi-informasi yang salah tersebut. Sehingga perlu diupayakan peluang dari kebenaran informasi tersebut seoptimal mungkin, atau peluang kesalahannya sekecil mungkin.



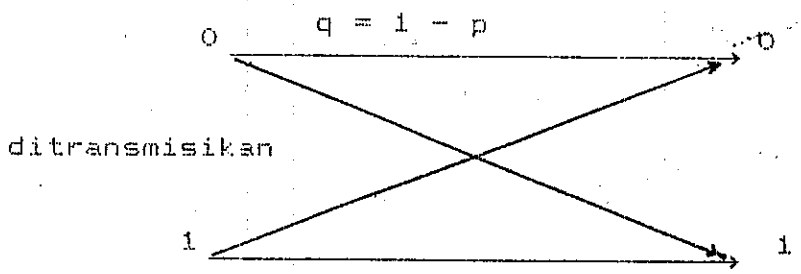
GAMBAR SKEMA TRASMISI SANDI LINIER

PADA CHANNEL SIMETRIS BINER

Defunisi 3.1.1

Channel simetris biner adalah suatu channel yang dilalui berita yang berupa sinyal bilangan 0 dan 1 dimana peluang dari angka 1 berubah menjadi 0 sama dengan angka 0 berubah menjadi 1. Dinamakan simetris karena peluang

berubahnya 1 menjadi 0 sama dengan 0 menjadi 1. Dan dinamakan biner karena sinyal-sinyal yang ditransmisikan adalah bilangan biner 0 dan 1.



GAMBAR SKEMA CHANNEL SIMETRIS BINER

Peluang tidak ada kesalahan yang terjadi bilamana ditransmisikan suatu k-digit berita adalah : q.q.q...q (sebanyak k) atau q^k .

Contoh :

1. Bila p = 0,001 dan ditransmisikan suatu berita 10.000 digit, maka peluang transmisi secara sempurna (tidak terjadi kesalahan) adalah :

   $q^k = (1-p)^k = (1-0,001)^{10.000} = 0,00005$

Selanjutnya akan ditunjukkan beberapa macam sandi yang peluang tidak terjadinya kesalahan cukup besar. Pada permasalahan sandi ini bilangan biner $w = w_1 \ldots v_n$ adalah elemen grup additif B^n, dan $W_i \in B = \{0,1\}$.

Bila bilangan biner yang ditransmisikan adalah :

$w = w_1 w_2 \ldots w_n$, dan bilangan biner yang diterima

$r = r_1 r_2 \ldots r_n$, maka pola kesalahan adalah bilangan biner $e = e_1 e_2 \ldots e_n$, dimana :

$$e = \begin{cases} 0, \text{ bila } w_i = r_i \\ 1, \text{ bila } w_i \neq r_i \end{cases}$$

Jadi angka 1 pada e merupakan angka-angka kesalahan yang terjadi pada w, pada waktu diterima sebagai r,sehingga posisi angka 1 pada e adalah posisi kesalahan yang terjadi selama transmisi sandi tersebut.

Contoh :

1. Bila pada pesawat penerima, diterima r = 010011101 dan diketahui pola kesalahan e = 001000100, maka didapatkan w = 011011001 dengan mengoreksi angka ketiga dan ketujuh pada r.

Sehingga didapat suatu persamaan dengan operasi penjumlahan bilargan biner grup additif $\mathbb{B}^n$.

1. w = r + e

   (Berita yang ditransmisikan = berita yang diterima + pola kesalahan).

2. r = w + e

   (Berita yang diterima = berita yang ditransmisikan + pola kesalahan).

3. e = w + r

   (Pola kesalahan = berita yang ditransmisikan + berita yang diterima).

Contoh :

1. Bila w = 01011010 dan r = 01111011, maka

   e = 00100001

2. Bila r = 111001001000 dan e = 000000001000, maka w = 111001000000.

Teorema 3.1.1.

Misal ditransmisikan suatu berita w n - digit melalui suatu channel simetris biner yang mana peluang kesalahan setiap digit adalah p.

a. Bila e adalah suatu pola kesalahan n - digit memuat angka 1 sebanyak k, maka peluang dari terjadinya e adalah $p^k (1-p)^{n-k}$.

b. Terdapat $\begin{bmatrix} n \\ k \end{bmatrix} = \frac{n!}{(n-k)!\,k!}$ pola kesalahan yang memuat angka 1 sebanyak k, sedemikian sehingga peluang yang tepat dari k kesalahan yang terjadi pada transmisi w adalah :

$$\begin{bmatrix} n \\ k \end{bmatrix} p^k (1-p)^{n-k}$$

Bukti :

a. Untuk pola kesalahan e sembarang, peluang dari setiap angka 1 yang terjadi adalah p sebanyak k dan peluang setiap angka 0 adalah 1 - p = q sebanyak n - k.

Disini proses terjadinya angka 0 tidak mempengaruhi proses terjadinya angka 1, dan misal peluang terjadinya angka 1 adalah P(A) dan peluang terjadinya angka 0 adalah P(B).

Dengan demikian peluang terjadinya angka 0 dan 1 adalah :

$$P(A \cap B) = P(A) \times P(B).$$

dimana : $P(A) = p^k$ dan $P(B) = q^{n-k} = (1-p)^{n-k}$

Sehingga :

$$P(A \cap B) = p^k \times q^{n-k} = p^k (1-P)^{n-k}$$

b. Jumlah pola kesalahan yang memuat 1 sebanyak k, sama dengan jumlah kombinasi dari n, untuk k kali, $\begin{pmatrix} n \\ k \end{pmatrix} = \dfrac{n!}{(n-k)!\, k!}$

Setiap dari $\begin{pmatrix} n \\ k \end{pmatrix}$ pola kesalahan mempunyai peluang $p^k (1-P)^{n-k}$.

Sehingga peluang yang tepat dari k kesalahan yang terjadi pada transmisi w adalah :

$$\begin{pmatrix} n \\ k \end{pmatrix} p^k (1-P)^{n-k}$$

Contoh :

1. Bila p = 0,01 dan ditransmisikan suatu berita 100 digit, peluang dari tidak terjadinya kesalahan adalah :

$$- \begin{pmatrix} n \\ k \end{pmatrix} P^o (1-p)^{n-o} = \begin{pmatrix} 100 \\ 0 \end{pmatrix} (0,01)^o (1-0,01)^{100}$$

$$= 1 \cdot 1 \cdot (0,99)^{100}$$

$$= 0,36603$$

- Peluang dari satu kesalahan adalah :

$$\begin{pmatrix} n \\ k \end{pmatrix} P^1 (1-p)^{n-1} = \begin{pmatrix} 100 \\ 1 \end{pmatrix} (0,01)^1 (1-0,01)^{100-1}$$

$$= 100 \cdot (0,01)(0,99)^{99}$$

$$= 0,36973$$

- Peluang dari dua kesalahan adalah :

$$\binom{n}{2} P^2 (1-p)^{n-2} = \binom{100}{2} (0,01)^2 (1-0,01)^{100-2}$$

$$= \frac{100.99}{2} (0,01)^2 (0,99)^{98}$$

$$= 0,18486$$

- Peluang lebih dari dua kesalahan adalah :

$$1 - \binom{n}{0} P^0 (1-p)^{n-0} - \binom{n}{1} p^1 (1-p)^{n-1} \binom{n}{2} p^2 (1-p)^{n-2}$$

$$= 1 - 0,36603 - 0,36973 - 0,18486$$

$$= 0,07938$$

Bila informasi yang akan ditransmisikan dalam bentuk sandi dalam digit yang panjang, sehingga untuk mengurangi adanya gangguan - gangguan yang akan menimbulkan terjadinya suatu kesalahan, serta untuk lebih mempermudah dalam pendeteksian dan pengoreksian seandainya terjadi suatu kesalahan. Maka sandi tersebut dibagi menjadi blok-blok sandi linier (n , m). Dalam hal ini sandi linier (n,m) dikirimkan dan diterima oleh suatu sistem yang terdiri dari fungsi penyandian (pembentuk sandi) = E (Encoding) dan fungsi pengurai sandi (pembaca sandi) = D (Decoding).

Definisi 3.1.2.

Fungsi Encoding E, didefinisikan dengan $E : \mathbb{B}^m \longrightarrow \mathbb{B}^n$, dimana E fungsi injektif dan $m < n$.

Definisi 3.1.3.

Fungsi Decoding D, didefinisikan dengan.

$D : \mathbb{B}^n \longrightarrow \mathbb{B}^m$,dimana D fungsi surjektif dan $m < n$

Definisi 3.1.4.

Kata sandi adalah sebarang elemen dari Im E (image dari E).

Definisi 3.1.4.

Suatu sandi (m , n) disebut suatu sandi linier, jika berita k-digit diubah oleh fungsi E menjadi kata sandi n - digit, dan fungsi E suatu transformasi linier.

Dalam suatu sandi linier (n , m), berita asli mempunyai panjang m - digit dan terdapat 2^m kemungkinan berita yang berbeda dan oleh sebab itu terdapat 2^m kata sandi. Sedang kata sandi yang diterima mempunyai n - digit, oleh sebab itu terdapat 2^n kemungkinan kata yang dapat diterima, tetapi hanya 2^m yang berupa kata sandi.

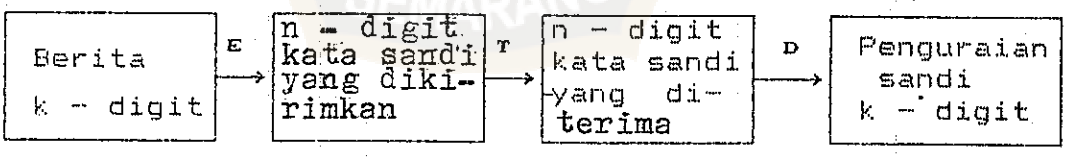
Dan n-k digit check ekstra yang ditambahkan untuk menghasilkan kata sandi disebut digit redundant, karena digit tersebut tidak mengandung informasi baru, tetapi hanya sebagai pelengkap informasi yang ada, untuk menjaga kerahasiaan berita yang dikirimkan.

Contoh

1. Sandi linier (9,3) adalah {000000000,100100100, 010010010,001001001,110110110,101101101,011011011 111111111}
2. Sandi linier (3,2) adalah {000,011,101,110}

Dari suatu berita yang panjang yang akan ditransmisikan, berita tersebut dipecah menjadi blok-blok sepanjang m. Kemudian fungsi Encoding membentuknya menjadi sandi kedalam blok-blok dengan panjang n. Dimisalkan E satu-satu, sehingga tidak' ada dua blok berita mempunyai kata sandi yang sama. Channel T mentransmisikan setiap digit, dengan peluang kesalahan P, dan D menguraikan sandi blok-blok sandi yang diterima, kedalam blok-blok dengan dengan panjang m, E dan D dipilih sedemikian hingga peluang bahwa suatu blok sandi yang telah diuraikan akan sama dengan blok berita asli, mendekati 1.

Adapun skema transmisi suatu sandi linier (n,m)



Untuk lebih effisien pengiriman suatu sandi linier (n,m), perlu diperhatikan dua hal :

1. Dipilih suatu sandi yang effisien, sehingga tidak ada pengiriman sandi dengan digit terlalu panjang atau terlalu pendek. Dalam hal ini $R = \frac{m}{n}$ (angka perbandingan sandi) harus mendekati 1.Sebab bila R merupakan bilangan rasional kecil, maka didalam

transmisi suatu sandi akan berisi banyak digit ekstra yang harus ditransmisikan, daripada digit berita itu sendiri. Sedang bila R merupakan bilangan rasional mendekati 1, maka untuk mentransmisikan suatu sandi hanya diperlukan sedikit digit ekstra untuk melengkapi digit dari berita yang akan dikirimkan.

$R = \frac{m}{n}$, adalah perbandingan banyak digit berita yang asli dengan banyak digit kata sandi yang dibentuk dari berita asli oleh fungsi E.

2. Fungsi E dan D dapat diemplementasikan secara praktis. Misal nya pada rangkaian elektronik digital yang digunakan untuk mengirimkan dan menerima informasi dalam bentuk sandi.

Jika nilai dari p kecil, maka kemungkinan besar suatu sandi akan dikirim tanpa suatu kesalahan, dan bila terjadi kesalahan, maka kesalahan yang terjadi hanyalah kesalahan tunggal. Yang dimaksud kesalahan tunggal adalah kesalahan yang terjadi hanya pada satu digit. Dan diperlukan sandi pengkoreksi kesalahan tunggal, untuk menguraikan sandi secara benar. Sandi pengkoreksi kesalahan lebih dari satu, diperlukan bila nilai p cukup besar.

Contoh-contoh :

1. Sandi parity check (m + 1, m) merupakan suatu sandi pendeteksi kesalahan. Disini perlu dibentuk suatu fungsi penyandian dan perlu diperhatikan bagaimana fungsi tersebut digunakan untuk mendeteksi

kesalahan-kesalahan transmisi yang banyak jumlahnya. Didefinisikan

$E : \mathbb{B}^m \longrightarrow \mathbb{B}^{m+1}$, $E(a_1, a_2 \ldots a_m) = a_1 \ldots a_m a_{m+1}$

dimana $a_{m+1} = a_1 + a_2 + \ldots a_m$

Jadi a_{m+1} adalah bilangan 0 atau 1, tergantung apakah jumlah $a_1, a_2 \ldots a_m$ genap atau ganjil.

Sehingga suatu kesalahan tunggal akan terjadi pada setiap kata sandi dengan jumlah genap akan berubah menjadi jumlah ganjil pada saat diterima dan demikian pula sebaliknya.

Jadi jenis sandi ini hanya digunakan jika kesalahan ganda tidak mungkin terjadi.

Sebagai contoh yang lebih spesifik :

a. Pada pengiriman suatu berita 10.000-digit, dengan $p = 0{,}001$. Berita tersebut dibagi dalam 1000 blok 10-digit. Suatu blok tunggal 10-digit dikirim dalam bentuk sandi 11-digit.

   Peluang dari pengiriman tanpa terjadi kesalahan adalah

$$\Theta\, q'' = (1-P)'' = (1-0{,}001)''$$
$$= (0{,}999)'' = 0{,}989055$$

   Dengan theorema 3.1.1. peluang dari satu kesalahan yang terjadi adalah :

$$\Theta \begin{pmatrix} n \\ k \end{pmatrix} p^k (1-p)^k = \begin{pmatrix} 11 \\ 1 \end{pmatrix} (0{,}001)^1 (1-0{,}001)^{11-1}$$
$$= 11 \cdot (0{,}001) \cdot (0{,}999)^{10}$$
$$= 0{,}01089$$

Jadi peluang dari paling banyak terjadi satu kesalahan dalam suatu blok 11 digit adalah :

- 0,98055 + 0,01089 = 0,999945.

Sehingga peluang dalam pengiriman berita 10.000 digit dalam 1000 blok 10-digit tanpa kesalahan paling sedikit : $(0,999945)^{1000} = 0,946$

Dalam transmisi 18 diantara 19 semua kesalahan yang terjadi terdeteksi.

2. Sandi pengulangan tiga kali (3m,m), merupakan suatu sandi pengoreksi kesalahan yang lebih teliti. Fungsi pembentuk sandi hanya mengulangi setiap sandi m - digit sebanyak tiga kali

$E(a_1a_2\ldots a_m) = a_1a_2\ldots a_m a_1a_2\ldots a_m a_1a_2\ldots a_m$

Selama menguraikan sandi, fungsi $D : \mathbb{B}^{3m} \longrightarrow \mathbb{B}^m$ memilih suatu digit ke i, bilangan pada digit ke i tersebut paling tidak akan muncul dua kali didalam transmisi

Contoh yang lebih spesifik

a. Misal m = 3, maka E (010) = 010010010. Bila terjadi kesalahan tunggal pada digit ke 6, maka sandi yang diterima adalah : 010011010.

Hal ini akan diuraikan sebagai 010 karena digit pertama, ke 4 dan ke 7 semuanya sama yaitu 0. Digit ke 2, ke 5 dan ke 8 semuanya sama yaitu 1. Digit ke tiga dan digit kesembilan sama yaitu 0. Sehingga pengulangan sandi rangkap 3, dapat untuk mengoreksi kesalahan tunggal yang terjadi dalam transmisi. Misal suatu berita 10.000-digit,

dengan p = 0,001. Suatu digit d tunggal disusun menjadi ddd. Peluang bahwa berita ini dikirim tanpa kesalahan adalah :

- $q^n = (1-p)^n = (1-0,001)^3 = (0,999)^3 = 0,997003.$

Dan peluang terjadinya kesalahan tunggal adalah :

- $\binom{n}{k} p^k (1-p)^{n-k} = \binom{3}{1} (0,001)^1$

$(1-0,001)^{3-1}$

$= 3\ (0,001)\ (0,999)^2 = 0,002994.$

Sehingga peluang penguraian sandi secara benar dari 3 digit adalah

- 0,997003 + 0,002994 = 0,999997.

Karena ada 10.000 - digit, sehingga peluang dari penguraian sandi secara benar untuk seluruh berita adalah :

- $(0,999997)^{10.000} = 0,97.$

Dengan demikian sandi tersebut mempunyai 33 kesempatan dalam 34 pengiriman sandi yang benar. Jadi untuk mentransmisikan, diperlukan 30.000 -digit untuk memperoleh 10.000 digit seperti yang diinginkan.

3. Suatu sandi pengulangan lima kali (5m,m) dapat untuk mengoreksi kesalahan ganda. Dalam hal ini, misal ada berita/ informasi yang akan dikirimkan sebanyak 10.000 digit dengan p = 0,001.

Peluang dari penguraikan sandi secara benar suatu digit tunggal adalah :

$$- \binom{5}{0}(0,001)^{0}(1-0,001)^{5-0} + \binom{5}{1}(0,001)^{1}$$

$$(1-0,001)^{5-1} + \binom{5}{2}(0,001)^{2}\ (1-0,001)^{5-2}$$

$$= (0,999)^{5} + 5(0,001)(0,999)^{4} + \frac{5.4}{2}(0,001)^{2}$$

$$(0,999)^{3} \quad 0,99999999.$$

Peluang dari ketelitian dalam penguraian sandi dari seluruh berita yang dikirimkan - $(0,99999999)^{10.000} = 0,9999$.

Sehingga peluang penguarian sandi secara salah dari seluruh berita hanya 1 diantara 10.000.

3.2. BEBAN DAN JARAK SANDI LINIER

Pada bagian ini akan dijelaskan mengenai beban jarak dari suatu sandi linier.

Definisi 3.2.1.

Beban dari suatu kata sandi $w = w_1 w_2 \ldots w_n$ untuk $w \in \mathbb{B}^n$ adalah banyaknya bilangan satu yang ada pada w, dan dinyatakan dengan $w_t(w) = w_1 + w_2 + \ldots + w_n$.

Contoh 3,2,1.

1. U = 101011. ,$w_t(U) = 4$
2. V = 110011 ,$w_t(V) = 4$
3. S = 100111001 ,$w_t(S) = 5$
4. t = 111000111 ,$w_t(t) = 6$.

Definisi.3.2.2.

Jarak dari dua kata sandi $U = U_1 U_2 \ldots U_n$ dan $V = V_1 V_2 \ldots V_n$, untuk $U, V \in \mathbb{B}^n$ adalah beban dari U + V dimana $U_i \neq V_i$, dan dinyatakan dengan $d(U,V) = w_t(U+V)$, $U_i \neq V_i$.

Contoh 3.2.2.

1. U = 101011, V= 110011.

   d (U,V) = 2

2. S = 100111001 , t = 111000111.

   d (s,t) = 7.

Definisi 3.2.3.

Jarak minimum dari sandi linier dalam $\mathbb{B}^n$ dinyatakan sebagai $d_{min} = \min (d(u,v))$, $u_i \neq v_i$, $u,v \in \mathbb{B}^n$.

LEMMA 3.2.1.

Bila $a,b,c \in \mathbb{B}^n$, maka $d(a,b) = d(b,a)$ dan $d(a,c) \leq d(a,b) + d(b,c)$. ($\mathbb{B}^n$ adalah ruang metrik dengan fungsi d).

Bukti : Misal $a = a_1 a_2 \ldots a_n$, $b = b_1 b_2 \ldots b_n$

dan $c = c_1 c_2 \ldots c_n$ dalam $\mathbb{B}^n$.

Karena $a + b = b + a$, maka :

$d(a,b) = w_t(a+b)$, $a_i \neq b_i = w_t(a_i + b_i)$, $a_i \neq b_i = d(b,a)$

jadi $d(a,b) = d(b,a)$

Didefinisikan $d(a_i, b_i) = w_t(a_i + b_i)$, $a_i \neq b_i$

dan didapatkan

$$d(a_i, b_i) = \begin{cases} 0 \text{ untuk } a_i = b_i \\ 1 \text{ untuk } a_i \neq b_i \end{cases}$$

sehingga

$$d(a_i, b_i) \leq d(a_i, b_i) + d(b_i, c_i)$$

Selalu benar untuk $a_i = c_i$

Selanjutnya bila $a_i \neq c_i$, $a_i \neq b_i$ atau $b_i \neq c_i$ didapatkan :

$$d(a,c) = \sum_{i=1}^{n} c(a_i,c_i)$$

$$\leq \sum_{i=1}^{n} d(a_i,b_i) + \sum_{i=1}^{n} d(b_i,c_i)$$

$$d(a,c) \leq d(a,b) + d(b,c)$$

Teorema 3.2.1.

Suatu sandi dapat mendeteksi semua pola kesalahan dengan beban $\leq k$ bila dan hanya bila jarak minimum antara kata-kata sandi tersebut paling kecil $k + 1$.

Bukti :

Misal fungsi Encoding $E : \mathbb{B}^m \longrightarrow \mathbb{B}^n$, sehingga dapat diketahui semua kata sandi yaitu $E(w) \in \mathbb{B}^n$. Dan misal kata sandi yang ditransmisikan adalah a dan $T(a)$ kata sandi yang diterima, dimana semuanya berada dalam $\mathbb{B}^n$, sehingga pola kesalahan $e = a + T(a)$, dan

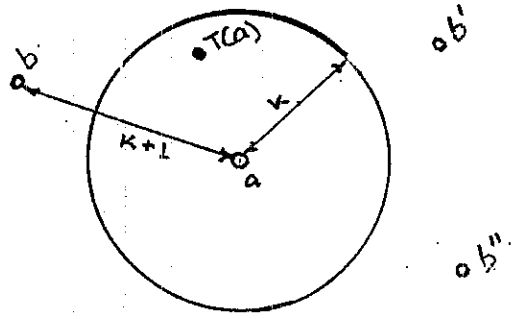
$$W_t(e) = W_t(a + T(a)) = d(a, T(a)) \leq k.$$

Kesalahan-kesalahan dalam transmisi dapat dideteksi, bila $T(a)$ bukan merupakan kata sandi. Yang dimaksud disini $T(a)$ bukan merupakan suatu kata sandi yang dikirimkan. Sehingga semua kesalahan dengan beban $e \leq k$ dapat dideteksi, bila dan hanya bila tidak ada kata sandi $b \neq a$ yang memenuhi $d(a,b) \leq k$. Berarti dalam hal ini untuk suatu kata sandi $b \neq a$ memenuhi.

$$d(a,b) > k \text{ atau } d(a,b) \geq k + 1$$

Jadi suatu k kesalahan dapat dideteksi apabila jarak antara kata sandi yang ditransmisikan : a dan kata sandi yang diterima: $T(a)$ tidak boleh lebih dari

k. Dan jarak minimum antara kata sandi paling sedikit k + 1.



Teorema 3.2.2.

a. Bila jarak minimum antara kata-kata sandi paling kecil 2K + 1, maka dapat dipilih suatu fungsi Decoding D yang akan mengoreksi semua pola kesalahan dengan beban ≤ k

b. Sebaliknya kata sandi yang berbeda a dan b mempunyai d(a,b) ≤ 2k, maka beberapa pola kesalahan dengan beban ≤ k tidak dapat dikoreksi.

Bukti :

a. Misal kata sandi yang ditransmisikan w dan kata sandi yang diterima r, dan kesalahan yang terjadi dalam transmisi paling banyak k sedemikian hingga :

$$w_t(e) = w_t(w+r) = d(w,r) \leq k.$$

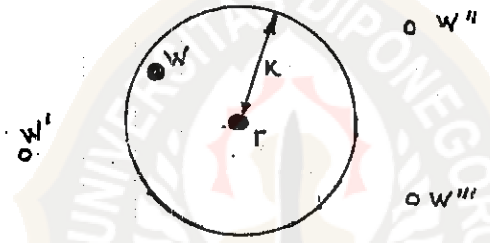
Kata sandi w dan r berada dalam $\mathbb{B}^n$ dan juga berada dalam bidang bola $s_k(r) = \{x \in \mathbb{B}^n \mid d(x,r) \leq k\}$. Bila w' kata sandi yang dikirimkan selain w, maka :

$$d(w,w') \leq d(w,r) + d(r,w') \leq k + k$$

karena $d(w,r) \leq k$; sehingga persamaan menjadi $d(w,w') \leq 2k < 2k + 1$.

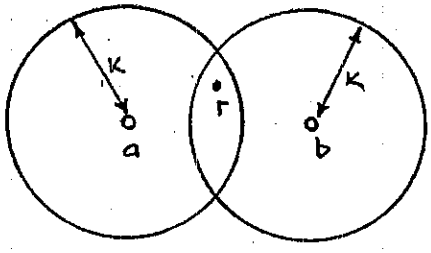
Kontradiksi dengan ketentuan bahwa untuk kata sandi yang berlainan, jarak minimum $2k + 1$ atau $d(w,w') \geq 2k + 1$. Sehingga dapat dipilih suatu fungsi D yang dapat mengoreksi semua pola kesalahan dengan beban $\leq k$.

$$D(r) = \begin{cases} w, \text{ bila kata sandi } w \text{ berada dalam } S_k(r) \\ \text{Sebarang, bila } S_k(r) \text{ tidak memuat kata sandi/bila terjadi lebih dari satu kesalahan pada } r. \end{cases}$$



b. Misal suatu sandi yang dikirimkan memuat kata sandi a dan b dengan jarak $d(a,b) \leq 2k$. Dan kata sandi yang diterima r, yang semuanya $\in B^n$ dengan $d(a,r) \leq k$ dan $d(b,r) \leq k$ (ambil $r_i = a_i = b_i$ bilamana $a_i = b_i$ dan pilih $r_i = a_i$ setengah kali jarak a_i dan b_i, bila $a_i \neq b_i$) Dalam hal ini D (r) tertentu, misal D (r) = a.

Maka bila b ditransmisikan dan diterima sebagai r dengan pola kesalahan $e = r + b$ dengan beban $\leq k$. Akan diuraikan/dibaca secara salah sebagai a



3.3. MATRIKS GENERATOR DAN MATRIKS PARITY CHECK.

Definisi 3.3.1.

Suatu matriks Generator G = [Im A] adalah suatu matriks m x n dimana m < n, dan Im matriks identitas m x m. Serta A matriks (m x (n-m)) .

Contoh 3.3.1

1. $\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$ adalah matriks Generator 3 x 3

Dengan menggunakan matriks Generator G, dapat ditetapkan suatu fungsi Encoding/Penyandian sebagai berikut:

$E(x) = X\,G$, untuk semua $x \in \mathbb{B}^m$....(3.3.1).

Contoh :

- Untuk $x = 110 \in \mathbb{B}^3$, maka

$$E(110) = 110 \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} = 110011 \quad \text{.....(3. 3. 3.)}$$

Sehingga secara umum untuk sembarang $a_1, a_2, a_3 \in \mathbb{B}^3$ diperoleh hasil sebagai berikut :

$$a_1\ a_2\ a_3 \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} = a_1\ \ a_2\ \ a_3\ \ (a_1+a_2)(a_1+a_3)(a_2+a_3)$$

Didalam $\mathbb{B}^6$. . . . . (3. 3. 4.)

Dengan demikian untuk membentuk suatu kata sandi dengan menggunakan matriks generatordalam fungsi Encoding menjadi sangat sederhana. Karena dengan mengalikan berita yang akan dikirim dengan matriks

generator dari sebelah kiri, maka didapatkan suatu kata sandi.

Apabila didalam transmisi dari kata sandi tersebut berjalan lancar dan tidak terjadi kesalahan, untuk menguraikan/membaca sandi tersebut juga dapat dilakukan dengan mudah. Karena kolom pertama dari matriks G adalah matriks identitas, sehingga berita yang dikirimkan hanyalah m digit pertama dari kata sandi tersebut.

Sedang dalam mengoreksi suatu kesalahan tidak dapat dilakukan oleh matriks generator sendiri.

Dari fungsi Encoding

$$E : \mathbb{B}^3 \longrightarrow \mathbb{B}^6$$

dimana :

$$E(a_1\ a_2\ a_3) = a_1\ a_2\ a_3\ a_4\ a_5\ a_6 \quad \ldots\ldots\ldots (3.3.5)$$

$a_4 = a_1 + a_2$, $a_5 = a_1 + a_3$, $a_6 = a_2 + a_3$

Dan karena $a_1, a_2, a_3, a_4, a_5, a_6 \in \mathbb{B}^6$, maka ketiga persamaan tersebut dapat ditulis sebagai :

$$\left.\begin{aligned} a_1 + a_2 + a_4 &= 0 \\ a_1 + a_3 + a_5 &= 0 \\ a_2 + a_3 + a_6 &= 0 \end{aligned}\right\} \quad \ldots\ldots (3.3.6)$$

Jadi simbol check a_4, a_5, a_6 ditentukan oleh a_1, a_2, a_3. Ketiga persamaan tersebut disebut persamaan parity-check. Dari ketiga persamaan parity-check, dapat dibentuk suatu matriks yang akan dipenuhi oleh setiap kata sandi $c = a_1\ a_2\ a_3\ a_4\ a_5\ a_6$.

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \quad \ldots\ldots(3.3.7)$$

Definisi 3.3.2.

Suatu matriks parity-check, yang berukuran (n-m) x n, n>m dimana n-m kolom yang terakhir adalah kolom-kolom dari matriks identitas yang berderajad n-m.

Contoh 3.3.2.

1. Matriks $H_{3\times 6} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$

Untuk sebarang berita $w \in \mathbb{B}^m$, maka kata sandinya tunggal $E(w) \in \mathbb{B}^n$.

Dimana m digit pertama adalah digit dari w, dan digit sisanya ditentukan oleh persamaan.

$$H. (E\ w)^T = 0 \quad \ldots\ldots\ldots\ldots(3.3.8)$$

Dari persamaan (3.3.4) dapat diperoleh n - m persamaan untuk n - m digit terakhir pada E w. Persamaan ke i menunjukan digit ke (m + i) darikata sandi yang diketahui. Dan dari persamaan (3.3.3) kata sandi yang terbentuk dan akan ditransmisikan adalah :

$$E(110) = 110 \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} = 110011$$

Andaikata pada suatu transmisi terjadi kesalahan pada digit ke 3, sehingga kata sandi yang diterima

r = 111011.

Sehingga untuk mengetahui letak kesalahan dapat dicari Sindromnya.

Definisi 3.3.3.

Bila H suatu matriks parity-check dan $r \in B^n$, merupakan kata sandi linier (n,m), maka $H.r^T = S$ disebut Sindrom dari r.

Contoh 3.3.3.

1. Misal r = 111011 dan matriks parity-check :

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Sindromnya adalah :

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$$

Pada proses diatas terlihat bahwa Sindrom S, sama dengan kolom ke-3 dari matriks parity-check. hal ini memberi petunjuk bahwa kesalahan yang terjadi pada transmisi ada pada digit ke 3 dari r. Sehingga dengan mengoreksi digit ke 3 dari r, dapat diketahui kata sandi yang dikirimkan adalah : C = E (w) = 110011, dan r dapat dibaca sebagai (w) dan beritanya adalah 110.

Pendeteksian kesalahan ini dapat dilakukan, mengingat bahwa untuk setiap kata sandi c, $H \cdot c^T = 0$ sesuai persamaan (3. 3. 8). Karena r = c + e, dimana e = 000... 010 ... 000 (digit ke i adalah 1)

merupakan pola kesalahan, bila digit ke i dari r terjadi kesalahan.

Sehingga didapatkan :

$$H.r^T = H\,(c + e)^T$$

$$= H.\,c^T + H.e^T = 0 + H.e^T \quad \ldots(3.3.9)$$

$$= \text{kolom ke i dari } H.$$

Jadi untuk sebarang pola kesalahan dengan beban 1 kata sandi akan dibaca/diterjemahkan secara benar..

Untuk selanjutnya akan dibahas apabila terjadi kesalahan ganda pada kata sandi. Bila berita $011 \in \mathbb{B}^3$ dengan $E : \mathbb{B}^3 \longrightarrow \mathbb{B}^6$

dan matriks $G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$

Sehingga matriks $H = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$

Dan kata sandi yang ditransmisikan :

$$c = E\,(011) = 011 \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} = 01110$$

Misal pola kesalahan e = 100100, sehingga kata sandi yang diterima adalah : r = c + e = 011110 + 100100 = 111010. Dengan demikian Sindromnya :

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$$

Sindrom sama dengan kolom 5 dari matriks H, sehingga timbul dengan bahwa suatu kesalahan tunggal terjadi pada digit ke 5 dari r, dengan pola kesalahan 000010. Dengan demikian kata sandi tersebut akan dibaca/diterjemahkan secara salah.

Atau bila pola kesalahannya adalah 001001, sehingga kata sandi yang diterima adalah r = c + e = 0111110 + 001010 = 010100

dan Sindromnya :

$$\begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

Sindrom diatas bukan merupakan salah satu kolom dari matriks H, dan sindrom tersebut merupakan jumlah dari kolom ke 1 dengan kolom ke 6, atau kolom ke 2 dengan kolom ke 4, atau kolom ke 3 dengan kolom ke 5. Sehingga timbul dugaan terjadi kesalahan pada dua digit (kesalahan ganda), dengan pola kesalahan 100001 (tidak benar), 010100 (tidak benar), atau 001010 (benar). Jadi apabila terjadi suatu kesalahan ganda, maka kata sandi yang akan dibaca/diterjemahkan akan salah.

Dengan demikian dapat dirumuskan suatu prosedur secara umum pendeteksian kesalahan sandi dengan matriks parity-check. Bila suatu kata sandi n - digit r = r_1 r_2 .....r_m .....r_n diterima, maka sindrom akan dapat dicari atau dihitung sebagai berikut :

$$H \cdot r^T = S \quad \ldots\ldots\ldots \quad (3,3,10)$$

Dalam hal ini ada 3 ketentuan :

1. Bila S = 0, trasmisi dari suatu kata sandi adalah benar, atau tidak terjadi kesalahan. Sehingga r adalah kata sandi yang dikirimkan dan berita asli adalah $r_1\ r_2\ \ldots\ldots r_m$.
2. Bila S = kolom ke i dari matriks H, mak suatu kesalahan tunggal terjadi pada digit ke i sehingga kata sandi yang dikirimkan adalah C = (r dengan digit ke i dikoreksi) dan berita asli adalah m digit pertama dari r.
3. Bila S bukan 0 dan bukan pula suatu kolom dari matriks H, maka paling sedikit terjadi kesalahan ganda dalam transmisi. Dan kesalahan ini tidak dapat dikoreksi.

Teorema 3.3.1.

Suatu matriks parity-check H (n-m) x n akan membaca semua kesalahan sandi tunggal secara benar bila dan hanya bila semua kolom dari matriks H bukan nol dan berlainan.

Bukti

(==>)

- Bila suatu kolom dari matriks H, katakan kolom ke i adalah 0, pola kesalahan adalah 0 .....010 .....0 (digit ke i adalah i) dan c adalah sembarang kata sandi yang dikirimkan, maka :

$$H.\ (\ c + e\ )^T = H.(c^T + e^T)$$

$$= H.c^T + H.e^T$$

$$= 0 + 0$$

$$= 0$$

Sehingga kesalahan tunggal yang terjadi pada digit ke i tidak terbaca.

- Bila kolom ke i = kolom j dari matriks H, pola kesalahan e adalah 0 ...010 ....0 (digit ke i adalah 1), dan c adalah kata sandi yang dikirimkan, maka :

$$H.(c + e)^T = H.(c^T + e^T)$$

$$= H.c^T + H.e^T$$

$$= 0 + H.e^T$$

$$= H.e^T = \text{kolom ke i} = \text{kolom ke j}$$

Dengan demikian kesalahan sandi yang terjadi tidak dapat diketahui digit mana yang salah, digit ke i atau digit ke j.

(<==)

- Sebaliknya, bila kolom-kolom dari matriks H bukan nol dan berlainan, maka dengan memperhatikan kedua hal tersebut diatas, membuktikan bahwa matriks H membaca sandi secara benar dan semua kesalahan sandi tunggal dapat dibaca.

Dengan kedua bukti diatas maka terbuktilah teorema diatas.

Teorema 3.3.2.

a. Bila A adalah suatu matriks m x (n-m) pada $\mathbb{B}$, sedemikian sehingga G = [Im A] adalah suatu matriks generator m x n, maka H = [A^T In-m] adalah

matriks parity-check tunggal untuk sandi yang sama.

b. Bila B adalah suatu matriks matriks (n-m) x m pada B, sedemikian sehingga H = [B I_{n-m}], maka G = [I_m B^T] adalah matriks generator tunggal untuk sandi yang sama.

Bukti

a. Dimisalkan matriks generator $G = [I_m\ A]_{m \times n}$, dan dari berita $w \in B^m$ dibentuk suatu kata sandi $wG \in B^n$ oleh suatu fungsi Encoding. Sehingga dari kata sandi yang dikirim dan didapatkan Sindromnya

$$\begin{aligned} H.(wG)^T &= H.(G^T + w^T) \\ &= (H.G^T).w^T = \left[(A^T\ I_{n-m}) \begin{bmatrix} I_m \\ A^T \end{bmatrix} \right] w^T \\ &= (A^T + A^T).w^T \\ &= 0.w^T \\ &= 0 \end{aligned}$$

Karena Sindrom = 0 dan m digit pertama dari wG adalah w, H sebagai matriks parity-check ikut menentukan pembentukan sandi, dari w ke wG. Sehingga G dan H berlaku pada sandi yang sama.

b. Sebaliknya, dimisalkan matriks parity-check H = $[B\ I_{n-m}]_{(n-m) \times n}$, matriks H menentukan suatu pembentukan sandi dari w ke kata sandi tunggal E (w), yang mana m digit pertamanya adalah w, dan dengan r - m digit sisa, sedemikian sehingga $H.(E(w)^T) = 0$. Tetapi m digit pertama dari WG adalah w, dan

$$H.\ (w.G)^T = H.(G^T.\ w^T)$$

$$= (H.G^T).\ w^T$$

$$= \left[(B\ I_{n-m}) \begin{bmatrix} I_m \\ B \end{bmatrix} \right].\ w^T$$

$$= (B + B).\ w^T = O.w^T$$

$$= O.$$

Sehingga $wG = E(w)$.

Dengan demikian perubahan pada G tentunya akan merubah sandi yang dibentuk oleh G. Jadi G tunggal untuk suatu sandi yang diberikan, dan dari bukti tersebut diketahui bahwa H menentukan G. Jadi H juga tunggal.

3.4. SANDI GRUP

Lemma 3.4.1.

Fungsi Encoding $E : B^m \longrightarrow B^n$ yang dibentuk oleh salah satu matriks Generator G atau suatu matriks parity-check H adalah suatu homomorphisma grup.

Bukti

- Untuk fungsi Encoding E yang diberikan oleh matriks Generator G, adalah pergandaan kanan oleh matriks G. Sehingga untuk suatu berita w dibentuk kata sandi E (w)

$$E(w) = wG \text{ didapatkan}$$

$$E(w_1 + w_2) = (w_1 + w_2)\ G$$

$$= w_1\ G + w_2 G$$

$$= E(w_1) + E(w_2)$$

Terbukti bahwa fungsi Encoding adalah morphisma grup.

- Untuk fungsi Encoding yang diberikan oleh matriks parity-check H, $E(\omega)$ adalah kata sandi yang mana m digit pertama adalah ω yang memenuhi : $H.E(\omega)^T = 0$. Oleh karena itu m digit pertama dari $E(\omega_1) + E(\omega_2)$ adalah $\omega_1+\omega_2$

sehingga,

$$H.(E(\omega_1) + E(\omega_2))^T = H.(E(\omega_1)^T + E(\omega_2)^T)$$

$$= H.E(\omega_1)^T + H.E(\omega_2)^T$$

$$= 0 + 0$$

$$= 0$$

Terbukti $E(w_1) + E(w_2) = E(w_1 + w_2)$.

Jadi fungsi Encoding adalah suatu homomorphisma grup.

Akibat 3.4.1.

Suatu sandi sebarang yang dihasilkan dari suatu matriks generator atau matriks parity-check adalah suatu sandi grup.

Bukti :

Menurut teorema 2.5.1. untuk suatu fungsi f : S $\longrightarrow$T, bila f suatu homomorfisma grup, maka S grup dan T juga grup.

Dan menurut Lemma 3.4.1. karena matriks G dan matriks H menentukan suatu fungsi Encoding, E : $\mathbb{B}^m \longrightarrow \mathbb{B}^n$ dimana E suatu homomorfisma grup, maka $\mathbb{B}^m$ suatu grup dan $\mathbb{B}^n$ juga merupakan suatu grup. Jadi suatu sandi yang dihasilkan oleh matriks H adalah suatu sandi grup.

Dari teorema 3.2.1. dan teorema 3.2.2. dapat diketahui bahwa kemampuan dari suatu sandi mendeteksi dan mengoreksi kesalahan-kesalahan tergantung pada jarak minimum diantara dua kata sandi.

Jarak minimum ini lebih mudah dihitung dari suatu sandi grup dengan menggunakan teorema berikut :

Teorema 3.4.1.

Dalam kata sandi grup, jarak minimum diantara kata-kata sandi adalah beban minimum dari suatu kata sandi yang bukan nol.

Bukti :

Misal d adalah jarak minimum diantara kata-kata sandi, dan d = d(a,b) dimana a dan b adalah kata-kata sandi yang berbeda. Misal w beban minimum dari suatu sandi yang bukan nol dan w = $w_t(c)$.

Akan dibuktikan d = w.

Karena a ≠ b, maka a + b ≠ 0.

Sehingga d = d(a,b) = $w_t(a+b)$ ≥ w .....(1)

Karena sebarang sub grup dari $\mathbb{B}^n$ memuat elemen identitas dari $\mathbb{B}^n$, maka 0 adalah suatu kata sandi dalam $\mathbb{B}^n$.

Sehingga :

$$w = w_t(c) = w_t(c+0) = d(c,0) \geq d \quad .....(2)$$

Dari persamaan (1) dan (2) didapatkan d = w.

Dengan demikian terbukti teorema ini.

Contoh :

1. Untuk suatu fungsi E : $\mathbb{B}^3 \longrightarrow \mathbb{B}^6$; dengan matriks

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$ membentuk sandi

000. G = 000000 ; 010. G = 010101 ; 110. G = 110011

001. G = 001011 ; 011. G = 011110 ; 111. G = 111000

Dimana beban dari kata-kata sandi tersebut adalah : 0,3,4,3,4 dan 3.

Dan beban minimumnya adalah 3. Sehingga dalam hal ini kata sandi mempunyai jarak minimum = 3.

3.5. PENGOREKSIAN SANDI DENGAN KOSET UTAMA

Setiap sandi grup yang diterima dari suatu transmisi dapat diuraikan dengan menggunakan tabel Decoding.

Dengan mengambil contoh yang dihasilkan oleh fungsi Encoding E : $\mathbb{B}^3 \longrightarrow \mathbb{B}^6$, dengan matriks generator

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

Yaitu :

000000 ; 001110 ; 010101 ; 100011 ; 011011 ; 101101 ; 110110 dan 111000.

Langkah I

Tulis semua kata sandi yang membentuk sandi grup C dalam satu baris, dengan 000... 00 pada kedudukan pertama.

000000 001110 010101 100011 011011 101101 110110 111000

Langkah II

Pilih salah satu kata sandi $x \in \mathbb{B}^n$, dalam hal ini $\mathbb{B}^n$ adalah $\mathbb{B}^6$, yang mempunyai beban paling kecil dan tulis pada posisi yang pertama. Dan tulis koset $x + c$ pada baris berikutnya. Sehingga $x + c$ terletak di bawah c, untuk setiap $c \in C$.

000000 001110 010101 100011 011011 101101 110110 111000

100000 101110 110101 000011 111011 001101 010110 011000

Langkah III

Ulangi langkah II sampai semua elemen dari $\mathbb{B}^n$ tertulis semua (karena koset-koset adalah kelas-kelas ekuivalensi pada $\mathbb{B}^n$, dan setiap elemen dari $\mathbb{B}^n$ digunakan tepat satu kali).

Langkah IV

Uraikan setiap kata sandi yang diterima sebagai mana kata sandi pada kolom yang sama, baris yang paling atas.

TABEL 3.5.1.

TABEL DECODING

000000	001110	010101	100011	011011	101101	110110	111000
100000	101110	110101	000011	111011	001101	010110	011000
010000	011110	000101	110011	001011	111101	100110	101000
001000	000110	011101	101011	010011	100101	111110	110000
000100	001010	010001	100111	011111	101001	110010	111100
000010	001100	010111	100001	011001	101111	110100	111010
000001	001111	010100	100010	011010	101100	110111	111001
010010	011100	000111	110001	001001	111111	100100	101010

Contoh :

1. Diterima kata sandi : 10010 001011 101010 001111 101111 101000 001000 011110

   Kemudian dicari letak kata sandi tersebut pada tabel 3.5.1. dan dilihat baris paling atas pada kolom yang sama dengan kata sandi yang diterima. Sehingga kata sandi tersebut diuraikan sebagai 110110 011011 111000 001110 111000 000000 dan 001110.

   Dan dapat disimpulkan bahwa berita asli yang dimaksud adalah ; 110, 011, 111, 001, 001, 111, 000 dan 001.

   Karena untuk setiap kata sandi, berita yang dimaksud adalah 3 digit yang pertama.

   X yang dipilih dari anggota $\mathbb{B}^n$ yang mempunyai beban paling kecil dan diletakkan pada kolom pertama setiap baris adalah koset utama pada masing-masing koset. Kadang-kadang terdapat suatu pilihan tunggal untuk koset utama ; seperti pada baris pertama sampai

baris ke tujuh pada tabel 3.5.1, koset utama adalah kata sandi tunggal dengan beban terkecil pada kosetnya. Tetapi pada baris ke 8, ada dua pilihan lain yang dapat digunakan sebagai koset utama dengan beban 2 selain 010010, yaitu 001001 dan 100100.

Penguraian sandi dengan dengan koset utama ini, selain memberikan suatu jawaban, untuk setiap kata sandi yang diterima. Teorema berikut menunjukkan bahwa methode ini selalu memberikan jawaban yang baik. Dan metode ini dapat digunakan untuk sandi pengoreksi kesalahan multipel.

Teorema 3.5.1.

Selama penguraian sandi dengan koset utama, setiap kata sandi yang diterima r diuraikan sebagai suatu kata sandi c sedemikian sehingga $d(r,c) \leq d(r,b)$, untuk semua kata sandi b.

Bukti

Misal b kata sandi selain c, dan x koset utama dalam koset utama dalam koset yang memuat r.

maka : $x = r + c$

$$d(r,c) = w_t(r + c) = w_t(x)$$

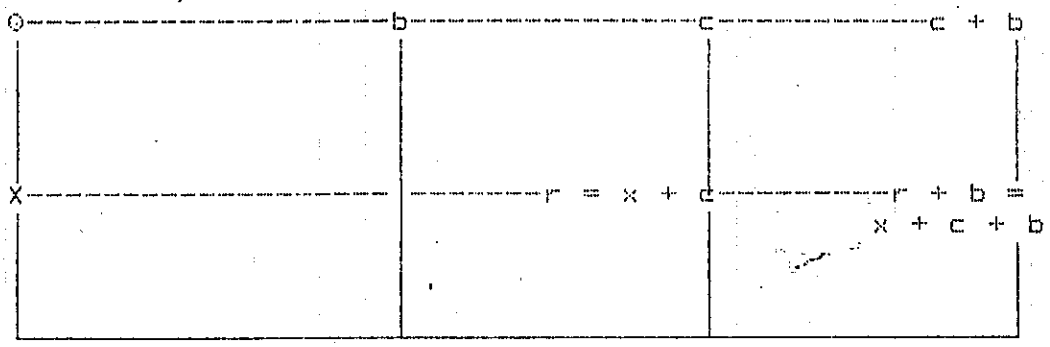
maka :

$$d(r,b) = w_t(r + b)$$

dimana $r + b = (x + c) + b$

$$= x + (c + b) \in x + C.$$

dan c adalah grup dari kata sandi. Dan bila dilihat pada Tabel 3.5.1 tampak seperti :



Karena x dipilih dari beban yang minimal pada kosetnya, maka $W_t(x) \leq W_t(r+b)$

Oleh sebab itu

$$d(r,c) = W_t(x) \leq W_t(r+b) = d(r,b)$$

Jadi $d(r,c) \leq d(r,b)$ terbukti.

Lemma 3.5.1.

Bila untuk suatu matriks parity-check H, sandi grup $C = \{c \in \mathbb{B}^n \mid H.c^T = 0\}$, maka kata-kata sandi x dan y dalam $\mathbb{B}^n$ pada koset yang sama bila dan hanya bila x dan y mempunyai Sindrom yang sama.

Bukti

X dan Y berada dalam koset yang sama

<===> $x = y + c$, untuk beberapa $c \in C$.

<===> $x + y =$, untuk beberapa $c \in C$.

<===> $x + y \in C$ (karena $c \in C$)

<===> $H.(X + Y^T) = 0$

<===> $H.(X^T + Y^T) = 0$

<===> $H.X^T + H.Y^T = 0$

<===> $H.X^T = H.Y^T$

Apabila ditambahkan Sindrom yang ditulis dalam bentuk baris pada sebelah paling kiri pada tabel 3.5.1. berubah menjadi Tabel 3.5.2.

Tabel 3.5.2.

TABEL DECODING DENGAN SINDROM

000	000000	001110	010101	100011	011011	101101	110110	111000
011	100000	101110	110101	000011	111011	001101	010110	011000
101	010000	011110	000101	110011	001011	111101	100110	101000
110	001000	000110	011101	101011	010011	100101	111110	110000
100	000100	001010	010001	100111	011111	101001	110010	111100
011	000010	001100	010111	100001	011001	101111	110100	111010
011	000001	001111	010100	100010	011010	101100	110111	111001
111	010010	011100	000111	110001	001001	111111	100100	101010

Bila penyusunan program suatu komputer dikerjakan dengan cara ini, hanya diperlukan untuk menyimpan dua kolom pertama dari Tabel 5.3.2, yaitu Sindrom dan koset utama dalam memory komputer.

Contoh :

1. Bila komputer menghitung Sindrom 011, dari kata sandi r yang diterima, dan akan diuraikan sebagai c = r + x. Dimana x = 100000, dengan demikian tinggal menjumlahkan 100000 dengan r untuk mendapatkan c.

   Penjelasan ini berdasarkan pada bilamana suatu kata sandi diuraikan oleh koset utama, maka pola-pola kesalahan yang mengoreksi adalah koset utamanya sendiri. Khususnya : penguraian sandi dengan koset utama akan mengoreksi semua kesalahan tunggal bila

dan hanya bila semua kata sandi dengan beban 1 adalah koset utama, dan akan mengoreksi semua kesalahan tunggal dan ganda bila dan hanya bila semua kata sandi dengan beban $\leq$ 2 adalah koset utama. Metode penguraian sandi ini sering digunakan untuk mengoreksi kesalahan ganda atau kesalahan rangkap tiga, bilamana dua kolom (Sindrom dan koset utama) tidak terlalu panjang untuk disimpan dalam memory komputer.